THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of verifying data integrity between at least two correspondents in a public-key cryptographic scheme, at least one of said at least two correspondents having a main processor and a secure module, said secure module being independent of said main processor's control, said method comprising the steps of:

assembling data on at least one of said at least two correspondents;

displaying data under control by said main processor to produce a first output;

displaying said data from said secure module to produce a second output;

comparing said first output and second output;

instructing said secure module to generate a signature upon a favorable comparison of said first output and said second output; and

whereby said favorable comparison indicates data integrity such that said at least one of said correspondents signs said data.

2. The method of claim 1, wherein said at least one of said at least two correspondents is a personalized device.

3. The method of claim 2, wherein said personalized device is a mobile phone.

4. The method of claim 2, wherein said personalized device is a personal digital assistant.

5. The system of claim 1, wherein said favourable comparison is characterized in that said first output and said second output are logically related to one another.

6. The system of claim 5, wherein said logical relationship is such that said first output and said output are identical.

7. The system of claim 1, wherein said step of displaying said data message includes displaying a portion of said data message.

8. The system of claim 7, wherein said favourable comparison is characterized in that a portion of said first output and a portion of said second output are logically related to one another.

9. The system of claim 8, wherein said logical relationship is such that said portion of said first output is identical to said portion of said second output.

10. A method of establishing a secure communication path for data between a personalized device and an user of said device in a PKI scheme, said device having a main processor and a secure module independently operative of said main processor, said method comprising the steps of:

providing an interface between said device and said user, said interface having an input device and an output device for providing a means for interaction between said user and device, said input device and output device controllable by said main processor;

providing a secure communication path between said secure module and a secure input device and a secure output device coupled thereto, said secure path logically isolated from any other communication path;

comparing said data displayed on said output device and said secure output device;

whereby said user of said personalized device can determine said integrity of said data based on said comparison.

11. The method of claim 10, wherein said user actuates said secure input device based only on said output of said secure output device.

12. A method for verifying the integrity of a data message between a correspondent and a personalized device in a communication system, each correspondent

adapted to receive and transmit data messages, said method comprising:

containing a secret key in said secure module, said secure module adapted to be removably coupled to said personalized device and communicatively coupled thereto;

controlling access to said personalized device.